REMARKS

Claims 1-21 are pending. Claims 1, 6-9, and 14-17 have been amended. Claims 1-21 remain in the application.

The drawings stand subject to objection for non-compliance with 37 CFR 1.84. In response, the specification has been amended to correct a clerical error. Corrections to the drawings are not required. Withdrawal of the objection to the drawings is requested.

Claims 1, 7-9, 14-17 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Claims 1, 6-9, and 14-17 have been amended. Withdrawal of the rejection for indefiniteness is requested.

Claims 1, 5-9, 13-17, and 21 stand rejected under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,088,804, issued to Hill et al., in view of U.S. Patent No. 6,357,008, issued to Nachenberg. Applicant traverses the rejection.

To establish a *prima facie* case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP § 2143.

A *prima facie* case of obviousness has not been established. The Hill patent discloses a method of operating a dynamic network security system to respond to a plurality of attacks on a computer network (Abstract). The system includes a plurality of security agents linked to a processor, which must first be trained to respond to attacks on the network (Col. 4, line 30 through Col. 5, line 6). In one embodiment, the security system is trained to respond to a plurality of training signatures that represent simulated network attacks (Col. 2, line 66 through Col. 3, line 3; Col. 6, lines 26-31; Col. 7, lines 9-17). A first attack signature is compared to each training signature to determine the training signature most closely resembling the first attack signature and the system is

adapted to respond by introducing the first attack signature as a new training signature (Col. 2, lines 4-16). In a second embodiment, security agents are configured to concurrently detect occurrences of security events characterizing a security attack and to process the security events to form attack signatures for display (Col. 3, lines 20-26). A trained processor is further configured to compare the attack signature to training signatures to determine which simulated attack most closely resembles the attack signature (Col. 3, lines 29-36). Finally, location identifiers identify the nodes in the network where security events may tack place (Col. 6, lines 1-3).

The Nachenberg patent discloses a method for detecting computer viruses through decryption, exploration and evaluation using emulation and artificial intelligence (Abstract; Col. 1, lines 16-20). During decryption, a sufficient number of instructions are emulated to allow an encrypted virus to decrypt the viral body of the encrypted virus (Col. 7, lines 3-5). During exploration, all sections of code within a region likely to contain any virus are emulated (Col. 7, lines 9-11). During evaluation, any suspicious operations observed during the decryption and exploration phases are analyzed to determine whether the target program appears to be infected by a computer virus (Col. 7, lines 17-20). Nachenberg also discloses static heuristic virus detection that involves searching the instructions of a target program of instruction sequences that perform operations typically used by computer viruses (Col. 2, lines 39-45).

First, the Hill and Nachenberg patents, taken as a whole, do not provide a suggestion, motivation, or reason to combine. Hill and Nachenberg are directed to solving different types of needs for respectively detecting network attacks versus detecting computer viruses. Hill teaches an approach to responding to network attacks that first requires training the system to respond to a plurality of training signatures (Col. 2, lines 66 through Col. 3, line 2; Col. 6, lines 26-31; Col. 7, lines 9-17). A network attack attempts to compromise a network by effecting the operation of one or more individual computer nodes. Hill teaches a processor detecting a plurality of security events occurring substantially concurrently within a given sampling period sufficient to form an attack signature

(Col. 1, lines 11-34; Col. 5, lines 29-38). In contrast, a computer virus primarily effects the operation of an single computer system. Nachenberg teaches dynamically detecting computer viruses in a target program by decryption, exploration and evaluation performed on the potentially-infected computer system (Col. 5, lines 28-40; Col. 6, line 66 through Col. 7, line 22). A CPU emulator executes files in a fully contained virtual environment, which is effectively isolated from the actual hardware devices to avoid harm while a file is being simulated (Col. 6, lines 51-58). One of ordinary skill in the art at the time of applicant's invention would not be motivated or have a reason to combine the network attack detection teachings of Hill with the computer virus detection teachings of Nachenberg. Hill relies on detecting security events that *actually* occurred concurrently on a plurality of nodes during a given sampling period, whereas Nachenberg relies on isolated file simulation performed *in isolation from* the system being protected. Nor does Hill provide any suggestion to combine the teachings of detecting actual security events with the actual security event detection as taught by Nachenberg.

In addition, Hill and Nachenberg employ incompatible approaches to solving their respective needs. Hill teaches network attack detection and response by relying on a database of simulated attacks (Col. 5, lines 29-31). The processor learns from accumulated training signatures to provide predictions of attacks that may occur on the network (Col. 5, lines 23-25; Col. 6, line 23 through Col. 7, line 46). In contrast, Nachenberg teaches computer virus detection by emulating a target program in a virtual environment and observing the simulated instructions for virus-like operations (Col. 3, lines 62-65). One of ordinary skill in the art at the time of applicant's invention would not be motivated or have a reason to combine the retrospective teachings of Hill with the prospective teachings of Nachenberg. Hill relies on *learned* attack signatures to which an attack signature is compared and matched, whereas Nachenberg performs emulation and observation to detect suspicious behavior without reference to learned or previously encountered behaviors. Nor does Hill provide any suggestion to combine the teachings of attack signature training with the virtual emulation and

observation environment as taught by Nachenberg.

Second, even when combined by picking and choosing selected parts, the Hill and Nachenberg patents do not teach or suggest all claim limitations when considered in light of the disclosure of each respective patent. Hill teaches processing security events to form attack signatures for use in network attack detection (Col. 5, lines 7-9 and 23-25). The security events may include port scans, malicious software, penetration attempts, and others that are included either through a specific code signature or through actions or attempts at actions (Col. 4, lines 37-41). Nachenberg teaches static heuristic virus detection involving searching the instructions of a target program for sequences that perform operations typically used by computer viruses (Col. 2, lines 39-45). Thus, Hill and Nachenberg fail to teach or suggest dynamically identifying each occurrence of a specific event sequence characteristic of behavior of a computer virus and the application which performed the specific event sequence, per Claims 1, 9 and 17.

Moreover, Hill and Nachenberg teach away from dynamically detecting computer viruses through associative behavioral analysis of runtime state, per Claims 1, 9 and 17. Hill teaches detecting network events based on predictions of *observed* attack signatures formed from security events, whereas Claims 1, 9 and 17 define dynamically detecting computer viruses by analyzing behavior that can include both illegitimate actions performed by a computer virus and legitimate actions performed by the application. Likewise, Nachenberg teaches static and dynamic virus detection involving searching target program instructions and emulating target program instructions, respectively, whereas Claims 1, 9 and 17 recite tracking a sequence of execution of monitored events and identifying specific event sequences characteristic of computer virus and application behaviors. Thus, Hill is training- and not dynamic behavior-based and neither Hill nor Nachenberg dynamically analyze computer virus and application behaviors.

Finally, if combined, the Hill and Nachenberg patents do not provide a reasonable expectation of success. When combined, Hill and Nachenberg would provide an inoperative result. Hill teaches detecting network attacks by

comparing an attack signature observed over a sampling period using a database of training signatures. Nachenberg teaches decrypting, exploring and evaluating sections of code in a target program in a virtual environment for suspicious behavior. In combination, the teachings of Nachenberg provide computer virus detection on individual computer systems that could be combined with the teachings of Hill as attack signatures, but would fail to include the broader range of security events also taught by Hill. Moreover, such a combination would still be limited to providing network attack detection based on trained, retrospective knowledge, and not dynamic associative behavior, per Claims 1, 9 and 17. Furthermore, such a combination would fail to dynamically analyze computer virus and application behaviors, especially since the location identifiers taught by Hill only identify where events may take place, but not what application is causing such events, per Claims 1, 9 and 17.

Thus, a *prima facie* case of obviousness has not been shown with respect to Claims 1, 9 and 17. Claims 5-8 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 13-16 are dependent on Claim 9 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claim 21 is dependent on Claim 17 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 1, 5-9, 13-17, and 21 for obviousness under 35 U.S.C. 103(a) is requested

Claims 2-4, 10-12, and 18-20 stand rejected under 35 U.S.C. 103(a) as being obvious over Hill et al., in view of Nachenberg, and further in view of U.S. Patent 6,279,113, issued to Vaidya. Applicant traverses the rejection.

As argued above with respect to the rejection of Claims 1, 5-9, 13-17, and 21 for obviousness over Hill et al., in view of Nachenberg, a *prima facie* case of obviousness has not been shown. Claims 2-4 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 10-12 are dependent on Claim 9 and are patentable for the above-stated reasons, and as further distinguished by the

limitations recited therein. Claims 18-20 are dependent on Claim 17 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Claims 1-21 are believed to be in condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: April 12, 2004

By: _____
Patrick J.S. Inouye, Esq.
Reg. No. 40,297

Law Offices of Patrick J.S. Inouye
810 Third Avenue, Suite 258
Seattle, WA 98104

Telephone: (206) 381-3900
Facsimile: (206) 381-3999